Information Security Policy

Introduction

The data stored in the Practice information systems represents an extremely valuable asset. It is therefore essential that all information processing systems under the Practice's responsibility must be protected to an adequate level from all likely events that may jeopardise confidentiality and threaten the security of data. Such events will include accidents as well as behaviour deliberately designed to cause difficulty and breaches of security.

Purpose

The purpose of the Policy is to preserve:

Confidentiality	Access to data is confined to those specifically authorised to view it.
Integrity	Data is timely and accurate and detected or amended only by those specifically authorised to do so.
Availability	Data is available to those authorised when it is needed.

Furthermore, the Policy's purpose is to raise the awareness of all Practice employees of the need to maintain and, where necessary, improve the security and confidentiality of systems and data.

Practising good systems security should minimise deliberate and accidental system breaches and in turn will assist in maximising system availability. It is recognised by the Practice that mistakes will happen and it is the intention of this Policy that staff should be supported in order to avoid such errors in the context of a 'security and confidentiality aware organisation'.

All staff are covered by a requirement to respect data confidentiality in their contract of employment with the Practice. Deliberate breaking of confidentiality and security rules is contrary to the contract of employment and this policy and is considered a disciplinary matter.

In order to reinforce and support awareness and responsibility on confidentiality and security, appropriate training and guidance is given to staff.

It is recognised, that whilst the principles of confidentiality and security can be set out in a policy, some of the practical implications will change over time. Such changes may result from:

- Changes in technology.
- Legal changes accompanying the widespread use of electronic communications facilities.

- Changes to organisational structures.
- Changing working practices.

Protection of Information

Care should be taken to ensure that unintentional breaches of confidence do not occur. The following guidance must be adhered to:

- Each PC user must take responsibility for the security of equipment software and data in his / her care.
- PCs and / or other peripheral devices (printers etc) must be switched off when not in use.
- Computer games must not be loaded onto or played on PCs.
- Regular data backups must be taken (to provide contingency backup) and stored securely in the fireproof backup safe.
- Encrypted media must be used for backups.
- Regular checking / monitoring of PCs will be carried out.
- Unofficial, unauthorised or unlicensed software should not be loaded onto PCs.
- Private work, unless for training purposes, is disallowed on PCs.
- Private access to the internet is disallowed.
- Faulty PC / computer equipment should be notified to the IT lead.
- PCs should not be moved without approval from the Practice Manager.
- The NHS Net email system should not be used for personal email.
- Information should be accessed on a “need to know” basis only.

Email Security

Consider whether the content of emails should be pass-worded before sending.

Be sure you have the correct email address before you click ‘send’ as some email software will suggest similar addresses you have received before.

If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc) not carbon copy (cc).
Be careful using a group email address – check who is in the group and make sure you really want to send your email to everyone.

If you send a sensitive email from a secured address to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Fax Security

Consider whether sending personal/sensitive information, by a means other than fax is more appropriate, such as using secure email.

Make sure you only send the information that is required e.g. only the information **specifically** asked for.
Double check fax number.
Check the recipient has adequate security measures in place.

If the information is sensitive, ask the recipient to confirm that they are at the fax machine, ready to receive the document and there is enough paper in the machine.

Confirm that the whole document has been received safely.

Use a cover sheet – this will let anyone know who the information is for and whether it is confidential or sensitive, without having to look at the contents.

Other Security Measures

Shred or put in confidential waste bags. Secure bags.

Passwords

Passwords are an effective Information Technology security device, but only if kept secret.

- Passwords must be changed regularly (at least every three months).
- Passwords must where ever possible consist of at least six characters consisting of letters and digits.
- Passwords must be kept secret.
- Passwords must not relate to the user or the system being accessed.
- Re-use of passwords must be avoided.
- Passwords must not be written down (other than for contingency measures where they should be given to the Practice Manager in a sealed envelope and kept in a lockable cupboard).

Personnel

- All visitors and external staff not falling under the "well known and trusted" description should sign the visitors' book and the person they are meeting notified. Visitors must be accompanied at all times.

- All new staff must be made aware of the importance of IT security at induction.

Viruses

- Do not accept disks or programmes for use on PCs without first having them virus checked.
- Only use official and reliable software. All new software should be checked by NECS first.
- Re-check removable storage devices which have been used off-site for possible virus infection on their return.
- Write-protect removable storage whenever possible.
- If a virus is suspected report to the Practice Manager.

Backups

- Data must be protected by defined and controlled back-up procedures.
- Data must be backed up regularly.
- Adequate generations of backup data must be held.
- Backup data must be accorded the same security as live data.
- Backup data must be stored securely.
- Backup data must be tested and verified regularly.

Management of Security and Confidentiality

The management of the security of computer held data and computer systems within the Practice is the overall responsibility of the Practice Manager /IT Lead.

Any threat or actual breach of security should be reported immediately to the / Practice Manager/IT Lead or, if this is not possible, to one of the Practice partners.

Serious breaches involving personal data must be reported to the Information Commissioners Office within 72 hours.

Staff Induction and Training

Information security and confidentiality will be addressed at the recruitment induction stage and monitored during employment. This is in order to reduce the risks of human error, theft, fraud or misuse of facilities and to ensure that all staff are aware of information security threats and are equipped to support this Policy in the course of their work.

Individual Accountability

Every member of staff is personally accountable for the function they perform. Furthermore, under the Data Protection Act (1998), all staff members are personally responsible for their actions according to the law.

Incident Reporting

Notify the Practice Manager/IT Lead immediately if any member of staff is aware of any factors which could possibly result in:

- The disclosure of data to unauthorised persons
- Putting the integrity of any information technology system data at risk
- Making any information technology system unavailable to its users
- Causing any adverse impact on the Organisation
- Using the Practice computer system without authorisation for private use

ACTS/GUIDANCE COVERING SECURITY OF DATA
Data Protection Act (1984 & 1998)

The Data Protection Act (1984) requires the registration of data relating to individuals which is held on the computer. The Data Protection Act 1998 came into force in early 1999 and covers how information about living identifiable persons is used. The Data Protection Act 1998 applies to both manual and computerised records. For all such data it is essential to abide by eight principles which govern the care and use made of data.

The Principles of the Act

- The information to be contained in personal databases shall be obtained and processed fairly and lawfully.
- Personal data shall be held only for one or more specified lawful purpose(s).
- Personal data held for any purpose shall not be used or disclosed to unauthorised sources.
- Personal data shall be kept accurate and where necessary kept up to date.
- Personal data held for any purpose shall not be kept longer than is necessary.
- An individual shall be entitled at reasonable intervals and without undue delay or expenses to: access any such data held by the data user and where possible, to have such data corrected or erased.

- Appropriate security measures shall be taken against unauthorised access to or alterations, disclosure or destruction of personal data and against accidental loss or destruction of personal data.

The General Data Protection Regulations (GDPR) will supersede the Data Protection Act. The principles of GDPR are as follows:

Personal Data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specific explicit purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary kept up to date
- Kept for no longer than is necessary.
- Kept secured.

Computer Misuse Act

The Computer Misuse Act is concerned with provision for securing computer material against unauthorised access or modification. The Act has the force of law in the UK and introduced specific computer misuse criminal offences:

- Unauthorised access to computer materials;
- Unauthorised access with intent to commit or facilitate further offences;
- Unauthorised modifications of computer materials.

Persons guilty of computer misuse under this Act are liable on conviction to imprisonment for a period of up to 5 years or a fine or both.

The Human Rights Act

The Human Rights Act allows the public to defend their rights in UK courts and compels public organisations (e.g.The NHS) to treat everyone equally with fairness, dignity and respect.

The Common Law of Confidentiality

This law specifies that doctor/patient information must not normally be disclosed without consent unless disclosure is necessary for safeguarding of the patient or others or in the public interest.